

501 P1068 US00

日 本 国 特 許 庁
JAPAN PATENT OFFICE

11000 U.S. PRO
09/900584
07/06/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 7月12日

出 願 番 号

Application Number:

特願2000-211787

出 願 人

Applicant(s):

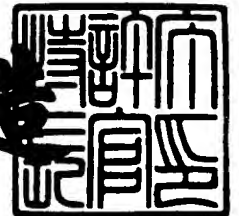
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月25日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 0000629106

【提出日】 平成12年 7月12日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/00

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 中野 雄彦

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【先の出願に基づく優先権主張】

【出願番号】 特願2000-205615

【出願日】 平成12年 7月 6日

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに記録媒体

【特許請求の範囲】

【請求項 1】 ネットワークを介して他の装置にコンテンツを送信する情報処理装置において、

前記コンテンツを暗号化する暗号化手段と、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証手段と、

前記認証手段の認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信手段と、

前記認証手段の認証結果に基づいて、前記他の装置の識別情報を取得する第 1 の取得手段と、

前記第 1 の取得手段により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する第 1 の計数手段と、

前記第 1 の計数手段により計数された前記識別情報を記憶する記憶手段と、

前記第 1 の計数手段により計数された前記受信台数の値に基づいて、前記認証手段の認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 前記認証手段の認証結果に基づいて、前記他の装置から受信台数の値を取得する第 2 の取得手段と、

前記第 2 の取得手段により取得された前記受信台数の値に基づいて、前記他の装置の受信台数を計数する第 2 の計数手段と

をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記送信手段により前記他の装置に送信された前記解除鍵が変更された場合、前記記憶手段により記憶された前記識別情報を消去するとともに、前記計数手段により計数された前記受信台数の値をリセットする情報更新手段を

さらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 ネットワークを介して他の装置にコンテンツを送信する情報処理装置の情報処理方法において、

前記コンテンツを暗号化する暗号化ステップと、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信ステップと、

前記認証ステップの処理による認証結果に基づいて、前記他の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項 5】 ネットワークを介して他の装置にコンテンツを送信する情報処理装置用のプログラムにおいて、

前記コンテンツを暗号化する暗号化ステップと、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、

前記認証ステップの処理による認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信ステップと、

前記認証ステップの処理での認証結果に基づいて、前記他の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶

制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 6】 第 1 のネットワークを介して第 1 の装置からコンテンツを受信する情報処理装置において、

前記第 1 の装置に対して、受信許可の要求を送信する第 1 の送信手段と、

前記第 1 の装置と認証する第 1 の認証手段と、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第 1 の装置から受信する受信手段と、

前記第 1 の装置から受信した前記コンテンツを、第 2 のネットワークを介して第 2 の装置に送信する第 2 の送信手段と、

前記第 2 の装置より受信許可が要求された場合、前記第 2 の装置と認証する第 2 の認証手段と、

前記第 2 の認証手段の認証結果に基づいて、前記受信手段により受信された前記解除鍵を前記第 2 の装置に送信する第 3 の送信手段と、

前記第 2 の認証手段の認証結果に基づいて、前記第 2 の装置の識別情報を取得する第 1 の取得手段と、

前記第 1 の取得手段により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する第 1 の計数手段と、

前記第 1 の計数手段により計数された前記識別情報を記憶する記憶手段と、

前記第 1 の計数手段により計数された前記受信台数の値に基づいて、前記第 2 の認証手段の認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項 7】 前記コンテンツを復号する復号手段と、

前記復号手段により復号された前記コンテンツを暗号化する暗号化手段と

をさらに備えることを特徴とする請求項 6 に記載の情報処理装置。

【請求項 8】 前記第 1 の認証手段の認証結果に基づいて、前記第 1 の計数手段により計数された前記受信台数の値を、前記第 1 の装置に送信する第 4 の送信手段と、

前記第 2 の認証手段の認証結果に基づいて、前記第 2 の装置から受信台数の値を取得する第 2 の取得手段と、

前記第 2 の取得手段により取得された前記受信台数の値に基づいて、前記第 2 の装置の受信台数を計数する第 2 の計数手段と

をさらに備えることを特徴とする請求項 6 に記載の情報処理装置。

【請求項 9】 前記第 3 の送信手段により前記第 2 の装置に送信された前記解除鍵が変更された場合、前記記憶手段により記憶された前記識別情報を消去するとともに、前記第 1 の計数手段により計数された前記受信台数の値をリセットする情報更新手段を

さらに備えることを特徴とする請求項 6 に記載の情報処理装置。

【請求項 10】 第 1 のネットワークを介して第 1 の装置からコンテンツを受信する情報処理装置の情報処理方法において、

前記第 1 の装置に対して、受信許可の要求を送信する第 1 の送信ステップと、

前記第 1 の装置と認証する第 1 の認証ステップと、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第 1 の装置から受信する受信ステップと、

前記第 1 の装置から受信した前記コンテンツを、第 2 のネットワークを介して第 2 の装置に送信する第 2 の送信ステップと、

前記第 2 の装置より受信許可が要求された場合、前記第 2 の装置と認証する第 2 の認証ステップと、

前記第 2 の認証ステップの処理による認証結果に基づいて、前記受信ステップの処理により受信された前記解除鍵を前記第 2 の装置に送信する第 3 の送信ステップと、

前記第 2 の認証ステップの処理による認証結果に基づいて、前記第 2 の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記第 2 の認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項 1 1】 第 1 のネットワークを介して第 1 の装置からコンテンツを受信する情報処理装置用のプログラムにおいて、

前記第 1 の装置に対して、受信許可の要求を送信する第 1 の送信ステップと、

前記第 1 の装置と認証する第 1 の認証ステップと、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第 1 の装置から受信する受信ステップと、

前記第 1 の装置から受信した前記コンテンツを、第 2 のネットワークを介して第 2 の装置に送信する第 2 の送信ステップと、

前記第 2 の装置より受信許可が要求された場合、前記第 2 の装置と認証する第 2 の認証ステップと、

前記第 2 の認証ステップの処理による認証結果に基づいて、前記受信ステップの処理により受信された前記解除鍵を前記第 2 の装置に送信する第 3 の送信ステップと、

前記第 2 の認証ステップの処理による認証結果に基づいて、前記第 2 の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記第 2 の認証ステップの処理での認証の成否を制御することにより、前記コンテン

ツの受信台数を制御する制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに記録媒体に関し、特に、コンテンツの利用を制限することができるようにした情報処理装置および方法、並びに記録媒体に関する。

【0002】

【従来の技術】

近年、インターネットに代表されるネットワークシステムが普及してきた。これにより、ユーザは、インターネットを介して情報を発信したり、あるいは、情報を受け取ったりすることができる。

【0003】

【発明が解決しようとする課題】

ところで、映画や音楽などの著作物の視聴を希望する利用者は、それに対する対価を支払うことにより、その著作物を受け取ることができる。

【0004】

しかしながら、インターネットなどのネットワークを通じて、映画や音楽などの著作物が、その所有者だけでなく、著作物に対する対価を支払っていない多くの利用者に対して、不正に視聴されてしまう恐れがあった。

【0005】

また、ネットワークを通じて不正に視聴される行為が無制限に行われるようになると、コンテンツ作成および流通ビジネスを阻害する恐れがあった。

【0006】

本発明はこのような状況に鑑みてなされたものであり、コンテンツが、ネットワークを介して、不正に利用されるのを防止することができるようにするものである。

【 0 0 0 7 】

【課題を解決するための手段】

本発明の第 1 の情報処理装置は、コンテンツを暗号化する暗号化手段と、他の装置より受信許可が要求された場合、他の装置と認証する認証手段と、認証手段の認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信手段と、認証手段の認証結果に基づいて、他の装置の識別情報を取得する第 1 の取得手段と、第 1 の取得手段により取得された識別情報に基づいて、コンテンツの受信台数を計数する第 1 の計数手段と、第 1 の計数手段により計数された識別情報を記憶する記憶手段と、第 1 の計数手段により計数された受信台数の値に基づいて、認証手段の認証の成否を制御することにより、コンテンツの受信台数を制御する制御手段とを備えることを特徴とする。

【 0 0 0 8 】

本発明の第 1 の情報処理装置は、認証手段の認証結果に基づいて、他の装置から受信台数の値を取得する第 2 の取得手段と、第 2 の取得手段により取得された受信台数の値に基づいて、他の装置の受信台数を計数する第 2 の計数手段とをさらに設けるようにすることができる。

【 0 0 0 9 】

本発明の第 1 の情報処理装置は、送信手段により他の装置に送信された解除鍵が変更された場合、記憶手段により記憶された識別情報を消去するとともに、計数手段により計数された受信台数の値をリセットする情報更新手段をさらに設けるようにすることができる。

【 0 0 1 0 】

本発明の第 1 の情報処理方法は、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理での認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信ステップと、認証ステップの処理による認証結果に基づいて、他の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶

制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【 0 0 1 1 】

本発明の第 1 の記録媒体に記録されているプログラムは、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理での認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信ステップと、認証ステップの処理による認証結果に基づいて、他の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【 0 0 1 2 】

本発明の第 1 の情報処理装置、第 1 の情報処理方法、および第 1 の記録媒体に記録されているプログラムにおいては、コンテンツが暗号化され、他の装置より受信許可が要求された場合、その受信を許可しても受信台数が許容値を超えない限り、他の装置と認証され、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵が他の装置に送信される。

【 0 0 1 3 】

本発明の第 2 の情報処理装置は、第 1 の装置に対して、受信許可の要求を送信する第 1 の送信手段と、第 1 の装置と認証する第 1 の認証手段と、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第 1 の装置から受信する受信手段と、第 1 の装置から受信したコンテンツを、第 2 のネットワークを介して第 2 の装置に送信する第 2 の送信手段と、第 2 の装置より受信許可が要求された場合、第 2 の装置と認証する第 2 の認証手段と、第 2 の認証手段の認証結果に基づいて、受信手段により受信された解除鍵を第 2 の装置に送信する第 3 の

送信手段と、第 2 の認証手段の認証結果に基づいて、第 2 の装置の識別情報を取得する第 1 の取得手段と、第 1 の取得手段により取得された識別情報に基づいて、コンテンツの受信台数を計数する第 1 の計数手段と、第 1 の計数手段により計数された識別情報を記憶する記憶手段と、第 1 の計数手段により計数された受信台数の値に基づいて、第 2 の認証手段の認証の成否を制御することにより、コンテンツの受信台数を制御する制御手段とを備えることを特徴とする。

【 0 0 1 4 】

本発明の第 2 の情報処理装置は、コンテンツを復号する復号手段と、復号手段により復号されたコンテンツを暗号化する暗号化手段とをさらに設けるようにすることができる。

【 0 0 1 5 】

本発明の第 2 の情報処理装置は、第 1 の認証手段の認証結果に基づいて、第 1 の計数手段により計数された受信台数の値を、第 1 の装置に送信する第 4 の送信手段と、第 2 の認証手段の認証結果に基づいて、第 2 の装置から受信台数の値を取得する第 2 の取得手段と、第 2 の取得手段により取得された受信台数の値に基づいて、第 2 の装置の受信台数を計数する第 2 の計数手段とをさらに設けるようにすることができる。

【 0 0 1 6 】

本発明の第 2 の情報処理装置は、第 3 の送信手段により第 2 の装置に送信された解除鍵が変更された場合、記憶手段により記憶された識別情報を消去するとともに、第 1 の計数手段により計数された受信台数の値をリセットする情報更新手段をさらに設けるようにすることができる。

【 0 0 1 7 】

本発明の第 2 の情報処理方法は、第 1 の装置に対して、受信許可の要求を送信する第 1 の送信ステップと、第 1 の装置と認証する第 1 の認証ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第 1 の装置から受信する受信ステップと、第 1 の装置から受信したコンテンツを、第 2 のネットワークを介して第 2 の装置に送信する第 2 の送信ステップと、第 2 の装置より受信許可が要求された場合、第 2 の装置と認証する第 2 の認証ステップと、第

2の認証ステップの処理による認証結果に基づいて、受信ステップの処理により受信された解除鍵を第2の装置に送信する第3の送信ステップと、第2の認証ステップの処理による認証結果に基づいて、第2の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、第2の認証ステップの処理での認証の成否を制御することにより、コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【0018】

本発明の第2の記録媒体に記録されているプログラムは、第1の装置に対して、受信許可の要求を送信する第1の送信ステップと、第1の装置と認証する第1の認証ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第1の装置から受信する受信ステップと、第1の装置から受信したコンテンツを、第2のネットワークを介して第2の装置に送信する第2の送信ステップと、第2の装置より受信許可が要求された場合、第2の装置と認証する第2の認証ステップと、第2の認証ステップの処理による認証結果に基づいて、受信ステップの処理により受信された解除鍵を第2の装置に送信する第3の送信ステップと、第2の認証ステップの処理による認証結果に基づいて、第2の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、第2の認証ステップの処理での認証の成否を制御することにより、コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【0019】

本発明の第2の情報処理装置、第2の情報処理方法、および第2の記録媒体に記録されているプログラムにおいては、第1の装置より第1のネットワークを介して受信したコンテンツが、第1の装置より得た許可台数を上限に、第2のネッ

トワークを介して第 2 の装置に送信される。

【 0 0 2 0 】

【発明の実施の形態】

図 1 は、本発明を適用したネットワークシステムの構成例を示すブロック図である。このネットワークシステムにおいては、ソース 1 が、バス 4 - 1 を介して、シンク 2 - 1 およびブリッジ 3 - 1 に接続され、また、ブリッジ 3 - 1 が、バス 4 - 2 を介して、シンク 2 - 2 およびブリッジ 3 - 2 に接続され、さらに、ブリッジ 3 - 2 が、バス 4 - 3 を介して、シンク 2 - 3, 2 - 4 に接続されている。

【 0 0 2 1 】

ソース 1 は、コンテンツを出力する出力装置である。コンテンツを出力する場合、ソース 1 は、コンテンツを暗号化した後、バス 4 - 1 乃至 4 - 3 を介して、シンク 2 - 1 乃至 2 - 4 に出力する。なお、暗号化されたコンテンツの復号に必要な鍵情報は、認証処理に成功したシンクにだけ渡される。これにより、コンテンツを受信するシンクの台数が制限される。なお、後述するブリッジ 3 - 1, 3 - 2 は、受信した信号を再出力するだけなので、台数カウントの対象から除外される。

【 0 0 2 2 】

シンク 2 - 1 乃至 2 - 4 (以下、シンク 2 - 1 乃至 2 - 4 を個々に区別する必要がない場合、単にシンク 2 と記載する。その他の装置においても同様とする) は、ソース 1 より供給されたコンテンツを受信する受信装置である。認証処理に成功した場合、シンク 2 は、ソース 1 より渡された鍵情報に基づいて、受信したコンテンツを復号する。ただし、ブリッジ 3 - 1 や 3 - 2 が暗号を一旦解き、新たな鍵で暗号化して出力する場合は、シンク 2 - 2 乃至 2 - 4 は直接つながるブリッジより渡された鍵情報に基づいて、受信したコンテンツを復号する。

【 0 0 2 3 】

ブリッジ 3 - 1, 3 - 2 は、ソース 1 より出力された、暗号化されているコンテンツを受信し、復号した後、再び暗号化してシンク 2 - 2 乃至 2 - 4 に出力するものとする。そのため、ブリッジ 3 - 1 は、ソース 1 と認証処理を行い、暗号

化されたコンテンツの復号に必要な鍵情報を取得するとともに、再出力するコンテンツを何台のシンク 2 に受信させたいかをソース 1 に伝える。そして、ブリッジ 3-1 は、ソース 1 から許可を得たら、ソース 1 に代わって、コンテンツを受信するシンク 2-2 乃至 2-4 の台数を制限する。なお、ブリッジ 3-2 は、ブリッジ 3-1 と認証し、同様にシンク 2-3, 2-4 の受信台数を制限する。

【 0 0 2 4 】

図 2 は、ソース 1 の詳細な構成例を示すブロック図である。

【 0 0 2 5 】

コンテンツプレーヤ 1 1 は、メディア 1 2 が装着されると、制御部 1 5 の制御に基づいて、メディア 1 2 に記録されているコンテンツを再生し、暗号部 1 3 に出力する。暗号部 1 3 は、コンテンツプレーヤ 1 1 より入力されたコンテンツを暗号化し、通信 I/F (インタフェース) 1 4 を介して、外部に出力する。なお、コンテンツプレーヤ 1 1 とメディア 1 2 の代わりに、放送コンテンツを受信し、出力するチューナーを持つソースも考えられる。

【 0 0 2 6 】

制御部 1 5 は、コンテンツプレーヤ 1 2、暗号部 1 3、通信 I/F 1 4、および記憶部 1 6 を制御する。制御部 1 5 はまた、コンテンツプレーヤ 1 1 で再生されたコンテンツを、必要に応じて、記憶部 1 6 に記憶させる。

【 0 0 2 7 】

図 3 は、シンク 2 の詳細な構成例を示すブロック図である。

【 0 0 2 8 】

制御部 2 4 は、画像・音声出力部 2 1、復号部 2 2、通信 I/F 2 3、および、記憶部 2 5 を制御する。制御部 2 4 はまた、通信 I/F 2 3 を介して送信されてきた、暗号化されているコンテンツを復号部 2 2 に送る。

【 0 0 2 9 】

復号部 2 2 は、通信 I/F 2 3 を介してソース 1 より送信されてきた鍵情報を取得する。復号部 2 2 はまた、コンテンツを、取得した鍵情報に基づいて復号する。画像・音声出力部 2 1 は、復号部 2 2 で復号されたコンテンツを出力する。

【 0 0 3 0 】

図4は、ブリッジ3の詳細な構成例を示すブロック図である。

【0031】

制御部35は、通信I/F31、復号部32、暗号部33、通信I/F34、および記憶部36を制御する。制御部35はまた、通信I/F31を介して送信されてきた、暗号化されているコンテンツを復号部32に送る。

【0032】

復号部32は、通信I/F31を介してソース1より送信されてきた鍵情報を取得するとともに、受信コンテンツを、取得した鍵情報に基づいて復号する。

【0033】

暗号部33は、復号部32で復号されたコンテンツを暗号化し、通信I/F34を介して、外部に出力する。

【0034】

なお、認証には、公開鍵暗号技術を用いるものとし、ソース1、シンク2、およびブリッジ3は鍵管理組織が発行する各機器用のDigital Certificate（以下、Certificateと記載する）と各機器用の秘密鍵と鍵管理組織の公開鍵を持つものとする。このCertificateには各機器用の秘密鍵と対応する各機器用の公開鍵、その機器の固有ID、そしてこの2つのデータに対する鍵管理組織による電子署名が含まれるものとする。

【0035】

図5は、ソース1とシンク2-1（図1）が、直接接続される場合の認証処理を説明する図である。

【0036】

まず、シンク1が自分のCertificateをソース2-1に送信する。具体的には、シンク1の制御部15が、記憶部16からCertificateを読み出し、通信I/F14を介して、ソース2-1に通信コマンドとして送信する（図5①）。

【0037】

ソース2は、この通信コマンドを受信すると、そのデータが正当なものか否かを判定する。具体的には、ソース2-1の制御部24が、記憶部25に記憶されている鍵管理組織の公開鍵を用いて、通信I/F23を介して受信したCertificate

中のデータと、それらに付随する鍵管理組織の電子署名が対応しているのか否かを調べる。すなわち、制御部 2 4 は、公開鍵暗号の DSA (Digital Signature Algorithm) Verify 演算処理を実行することにより、受信データの正当性を判定する。そして、判定結果が、正当である場合、認証処理を継続し、そうでない場合、認証処理を終了する。

【0038】

処理を継続する場合、ソース 1 の制御部 1 5 は、Certificate 中の相手の ID が記憶部 1 6 に保持する認証済み ID リスト（以下、ID リストと記載する）に登録済みであるか否かを調べ、登録済みの場合、変数 CntUp に 0 を代入する。

【0039】

一方、ID リストに Certificate 中の相手の ID が未登録の場合、ソース 1 の制御部 1 5 は、受信を許可したシンク 2 の数（以下、変数 SinkCnt と記載する）と受信を許可できる上限数（以下、変数 MaxSink と記載する）を比較し、変数 SinkCnt の方が小さければ変数 CntUp に 1 を代入する。

【0040】

なお、SinkCnt = MaxSink の場合、認証処理は終了される。また、変数 MaxSink は、変数でなくてもよい（すなわち、定数であってもよい）。

【0041】

そして、ソース 1 の制御部 1 5 は、擬似乱数生成アルゴリズムにより、擬似乱数 Random_challenge を生成し、シンク 2 に通信コマンドとして送信する（図 5 ②）。

【0042】

シンク 2 - 1 の制御部 2 4 は、この通信コマンドを受信すると、その値に対して、記憶部 2 5 に保持されている自分自身の秘密鍵を用いて、公開鍵暗号の DSAS ign 演算処理を実行して、電子署名を計算する。シンク 2 - 1 の制御部 2 4 は、計算された電子署名を、通信コマンド（Response データ）として、ソース 1 に送信する（図 5 ③）。

【0043】

ソース 1 の制御部 1 5 は、この通信コマンドを受信すると、自分が送った擬似

乱数Random_challengeとこの電子署名が対応しているか否か、すなわち、上述したDSA Verify演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取ったCertificate中の相手の公開鍵が用いられる。そして、判定結果が、正当である場合、認証処理が継続され、そうでない場合、認証処理は終了される。

【 0 0 4 4 】

処理を継続する場合、ソース 1 の制御部 1 5 は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク 2 - 1 に通信コマンドとして送信し（図 5 ④）、変数SinkCntの値を変数CntUpの値だけ増加する。そして、ソース 1 の制御部 1 5 は、Certificate中の相手のIDが記憶部 1 6 に保持する認証済みIDリストに登録済みであるか否かを調べ、登録済みの場合、変数CntUpに 0 を代入する。一方、IDリストにCertificate中の相手のIDが未登録の場合、変数SinkCntと変数MaxSinkを比較し、変数SinkCntの方が小さければ変数CntUpに 1 を代入する。

【 0 0 4 5 】

シンク 2 - 1 は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことによって、コンテンツを受信することができる。

【 0 0 4 6 】

また、図 1 に示されるソース 1 とシンク 2 - 2 のように、ソース 1 より出力されたコンテンツが、ブリッジ 3 - 1 を経由した後に、シンク 2 - 2 に受信される場合、やはり、シンク 2 - 2 とブリッジ 3 - 1 は、図 5 に示されたような認証処理を行う。すなわち、ソース 1 とシンク 2 - 3、または、ソース 1 とシンク 2 - 4 のように、2 台以上のブリッジ経由でコンテンツが伝送される場合でも、シンク 1 と最後のブリッジ 3 - 2（シンク 2 - 3、2 - 4 と直接つながるブリッジ）は同様の認証処理を行う。

【 0 0 4 7 】

以上の認証処理におけるシンク 2 の処理フローを図 6 に、ソース 1 の処理フローを図 7 に、それぞれ示す。

【 0 0 4 8 】

シンク 1 の認証処理は、相手がブリッジ 3 であっても、ソース 2 の場合と全く

同じである。ブリッジ3の認証処理は、図7のステップS15に示す処理が、ソース2の場合と異なる。具体的には、SinkCnt=MaxSinkの場合、ブリッジ3は、変数MaxSinkの値を大きくするために、自分自身が受信（入力）しているコンテンツの発信元であるソース1またはブリッジ3（図1の例の場合、ブリッジ3-1ならソース1、ブリッジ3-2ならブリッジ3-1）に受信許可を要求する認証処理を行う。なお、この場合には、1台以上の受信台数の追加が要求される。この認証処理が成功した場合、図7のステップS16以降の処理が継続される。

【0049】

図8は、ソース1とブリッジ3-1（図1）が、直接接続される場合の認証処理を説明する図である。

【0050】

まず、ブリッジ3-1の制御部35は、自分のCertificate、変数RelCntおよび変数AbsCntをソース1に送信する（図8①）。ここで、変数RelCntは、ブリッジ3-1が新たに得たい受信許可の台数を表わし、変数AbsCntは、既に得ている許可台数と今回許可を得たい台数の合計台数を表わしている。

【0051】

ソース1の制御部15は、これを受信すると、Certificateが正当なものか否かを、上述したDSA Verify演算処理を実行することにより判定する。そして、判定結果が、正当でない場合、認証処理は終了される。

【0052】

処理を継続する場合、ソース1の制御部15は、Certificate中の相手のIDが自分のIDリストに登録済みか否かを調べ、登録済みの場合、変数CntUpに変数RelCntを代入する。

【0053】

一方、IDリストにCertificate中の相手のIDが未登録の場合、ソース1の制御部15は、変数CntUpに変数AbsCntを代入する。そして、ソース1の制御部15は、変数SinkCntに変数CntUpを加えた値が、変数MaxSinkより小さいか否かを判定し、等しい場合、認証処理を終了する。

【0054】

そして、ソース 1 の制御部 1 5 は、擬似乱数 Random_challenge を生成し、ブリッジ 3 - 1 に通信コマンドとして送信する（図 8 ②）。

【 0 0 5 5 】

ブリッジ 3 - 1 の制御部 3 5 は、この通信コマンドを受信すると、その値と送信済みの変数 RelCnt と変数 AbsCnt に対して、記憶部 3 6 に保持されている自分自身の秘密鍵を用いて、上述した DSA Sign 演算処理を実行して、電子署名を計算する。ブリッジ 3 - 1 の制御部 3 5 は、計算された電子署名を、通信コマンド（Response データ）として、ソース 1 に送信する（図 8 ③）。

【 0 0 5 6 】

ソース 1 の制御部 1 5 は、この通信コマンドを受信すると、自分が送った擬似乱数 Random_challenge、受信済みの変数 RelCnt および変数 AbsCnt に、この電子署名が対応しているか否か、すなわち、上述した DSA Verify 演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取った Certificate 中の相手の公開鍵が用いられる。そして、判定結果が、正当でない場合、認証処理は終了される。

【 0 0 5 7 】

処理を継続する場合、ソース 1 の制御部 1 5 は、コンテンツにかけた暗号を解くのに必要な鍵情報をブリッジ 3 - 1 に通信コマンドとして送信し（図 8 ④）、変数 SinkCnt の値を変数 CntUp の値だけ増加させた後、相手の ID が ID リストに未登録の場合、追加する。

【 0 0 5 8 】

ブリッジ 3 - 1 は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解いた後、再び暗号化してコンテンツを出力する。そして、ブリッジ 3 - 1 の制御部 3 5 は、変数 MaxSink の値を変数 RelCnt の値だけ増加する。

【 0 0 5 9 】

以上の認証処理におけるブリッジ 3 の処理フローを図 9 に、またソース 1 の処理フローを図 1 0 に、それぞれ示す。

【 0 0 6 0 】

また、図 1 に示されるソース 1 とシンク 2 - 3、またはソース 1 とシンク 2 -

4のように、ソース1より出力されたコンテンツが、2台以上のブリッジ3-1、3-2を経由した後に、シンク2-3、2-4に受信される場合、やはり、コンテンツを出力するブリッジ3-1（以下、Txブリッジと記載する）とそれを受け取るブリッジ3-2（以下、Rxブリッジと記載する）は、図8に示されたような認証処理を行う。

【0061】

なお、Rxブリッジの認証処理は、相手がソース1の場合と全く同じである。

【0062】

Txブリッジの認証処理は、図10のステップS46に示す処理が、ソース1の場合と異なる。具体的には、 $\text{SinkCnt} + \text{CntUp} > \text{MaxSink}$ の場合、Txブリッジは、変数MaxSinkの値を大きくするために、自分自身が入力しているコンテンツの発信元であるソース1またはブリッジ3に受信許可を要求する認証処理を行う（図1の例の場合、ブリッジ3-1はソース1に認証を要求する）。なお、この場合には $(\text{SinkCnt} + \text{CntUp}) - \text{MaxSink}$ 以上の受信台数の追加が要求される。この認証処理が成功した場合、図10のステップS50以降の処理が継続される。

【0063】

また、他の処理例としては、変数RelCntおよび変数AbsCntが、Certificateとは別に送信される場合が考えられる。例えば、図8③に示されたResponseと共に送信する方法、あるいは、全く別の通信コマンドで送信する方法もある。

【0064】

また、図7のステップS15、または、図10のステップS46において、ブリッジ3-1、3-2が、新たに接続されたソース1かブリッジ3と認証を行う場合、その結果によらず、その後の処理は継続しない方法もある。すなわち、新たな認証は、次回以降の認証を成功させるためのものと位置付けることができる。

【0065】

さらにまた、シンク2が自分の出力を受けるのを止め、暗号を解くのに必要な情報を失った場合、ソース1またはブリッジ3は、変数SinkCntをそのシンク2の分だけ減らすことができる。例えば、ソース1やブリッジ3がコンテンツにか

ける暗号の鍵情報を変更したら、シンク2は、自分自身の変数SinkCntを0にすることができる。

【0066】

以上のように、ソース1またはブリッジ3が、出力を受けられるシンク2の受信台数を制限するようにしたので、以下に示すような効果が得られる。

(1) コンテンツに関する権利者は、コンテンツの不正視聴や記録を未然に防ぐことができる。

(2) ブリッジを使って信号を再出力した場合でも、ソースは、ブリッジの先にいるシンクも含め、台数を制限することができる。

(3) 台数の制限を機器固有のIDを使って行うことで、同じシンクが何度認証しても台数を誤って増やすことが無い。

(4) ブリッジが受信許可をソースや別のブリッジに要求する際に、受信台数の増加または減少分と受信合計台数を知らせることで、ソースや別のブリッジは、そのブリッジと認証したことがある場合、あるいは、認証したことがない場合のいずれにおいても、変数SinkCntを容易に、正しい値に変更することができる。

(5) 公開鍵暗号技術を用いることで、機器固有IDや要求台数を、安全に他の機器に渡すことができ、かつ、正しい台数管理を行うことができる。

【0067】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0068】

この記録媒体は、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク（MD (Mini-Disk) を含む）、もしくは

半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMやハードディスクなどで構成される。

【0069】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0070】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0071】

【発明の効果】

以上のように、本発明の第1情報処理装置、第1の情報処理方法、および第1の記録媒体に記録されているプログラムによれば、コンテンツを暗号化し、他の装置より受信許可が要求された場合、その受信を許可しても受信台数が許容値を超えない限り、他の装置と認証し、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信するようにしたので、コンテンツの利用を制限することが可能になる。

【0072】

また、本発明の第2の情報処理装置、第2の情報処理方法、および第2の記録媒体に記録されているプログラムによれば、第1の装置より第1のネットワークを介して受信したコンテンツを、第1の装置より得た許可台数を上限に、第2のネットワークを介して第2の装置に送信するようにしたので、出力コンテンツの受信装置を、得た許可台数に基づいて制限することが可能になる。

【図面の簡単な説明】

【図1】

本発明を適用したネットワークシステムの構成例を示すブロック図である。

【図2】

図1のソースの詳細な構成例を示すブロック図である。

【図3】

図1のシンクの詳細な構成例を示すブロック図である。

【図4】

図1のブリッジの詳細な構成例を示すブロック図である。

【図5】

ソースまたはブリッジとシンクの認証処理を説明する図である。

【図6】

シンクのソースまたはブリッジに対する認証処理を説明するフローチャートである。

【図7】

ソースまたはブリッジのソースに対する認証処理を説明するフローチャートである。

【図8】

ソースまたはTxブリッジのRxブリッジの認証処理を説明する図である。

【図9】

RxブリッジのソースまたはTxブリッジに対する認証処理を説明するフローチャートである。

【図10】

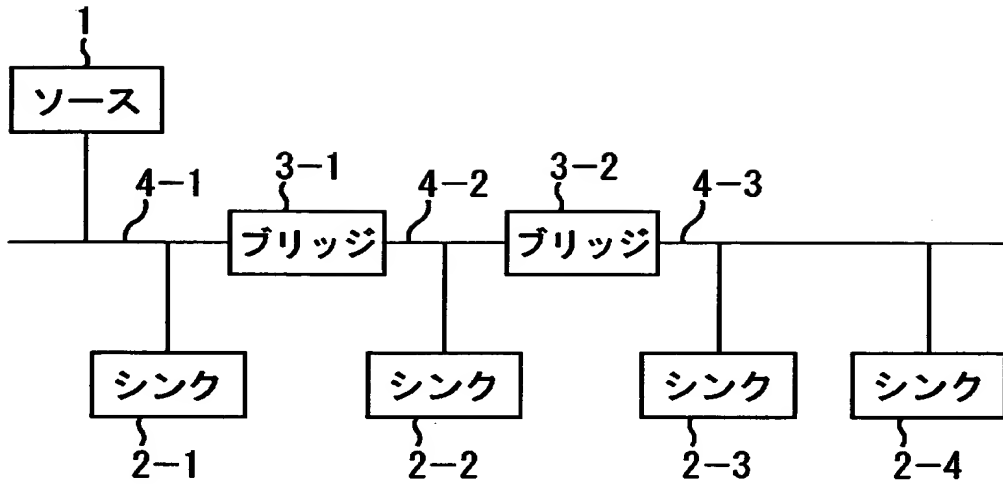
ソースまたはTxブリッジのRxブリッジに対する認証処理を説明するフローチャートである。

【符号の説明】

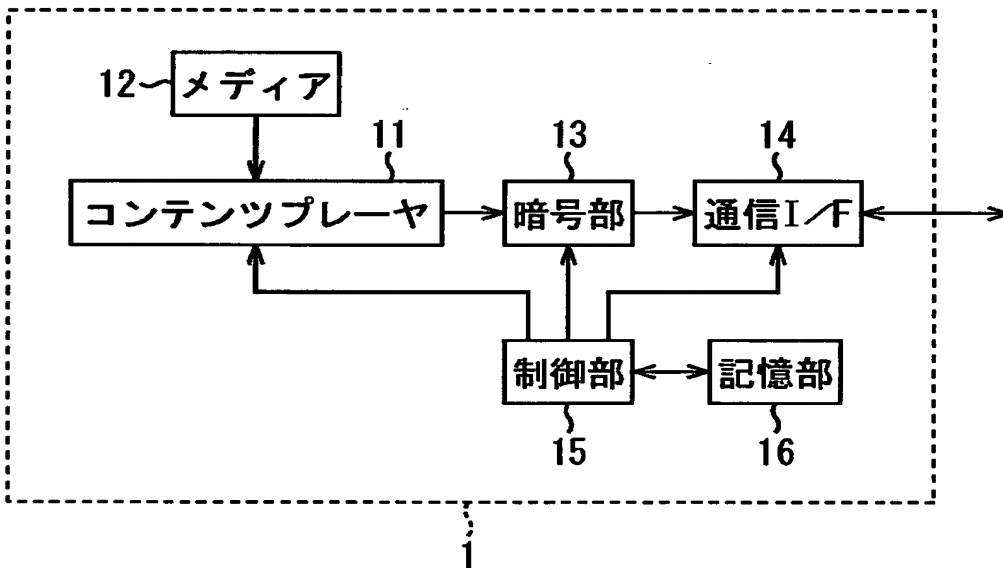
1 ソース, 2-1乃至2-4 シンク, 3-1, 3-2 ブリッジ, 11 コンテンツプレーヤ, 12 メディア, 13 暗号部, 14 通信I/F, 15 制御部, 16 記憶部, 21 画像・音声出力部, 22 復号部, 23 通信I/F, 24 制御部, 25 記憶部, 31 通信I/F, 32 復号部, 33 暗号部, 34 通信I/F, 35 制御部, 36 記憶部

【書類名】 図面

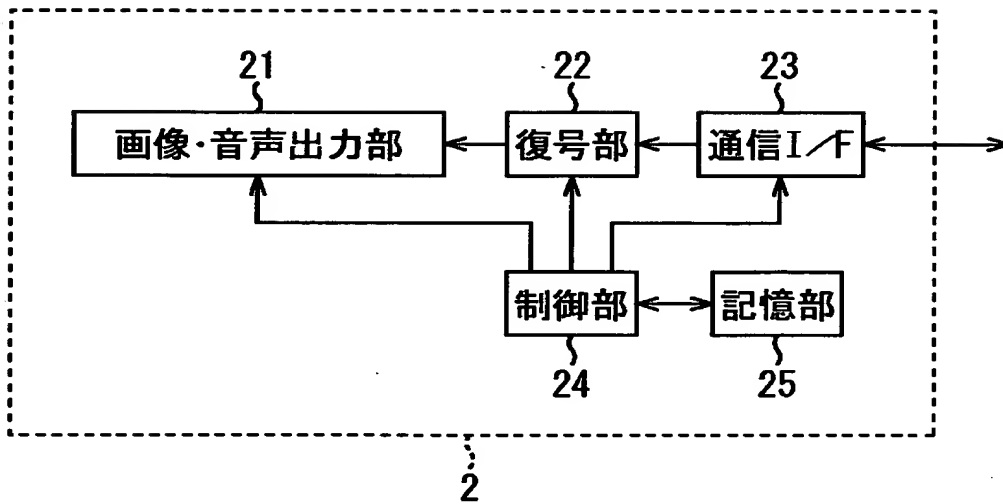
【図 1】



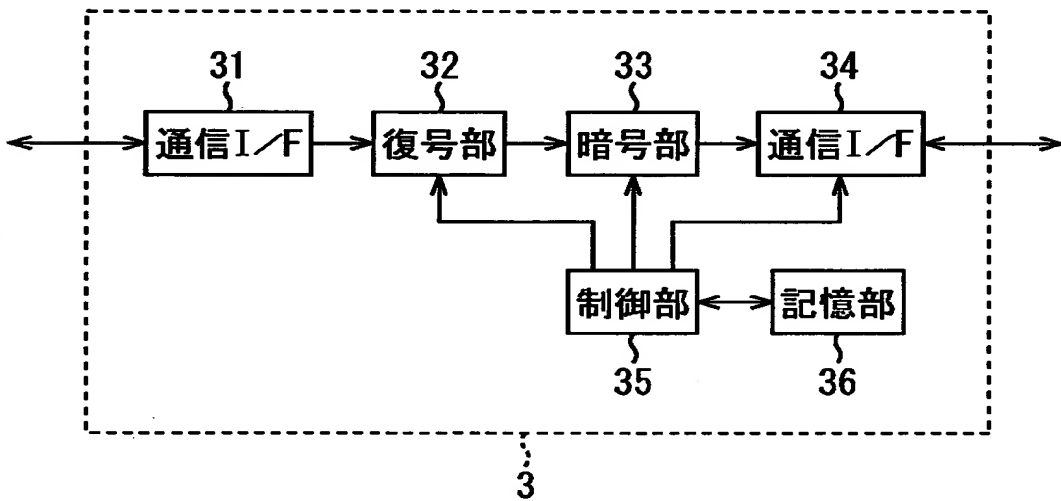
【図 2】



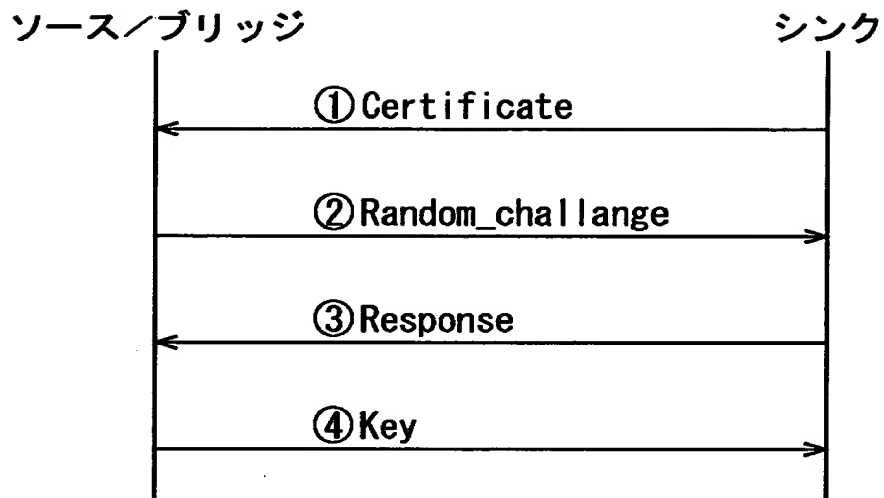
【図3】



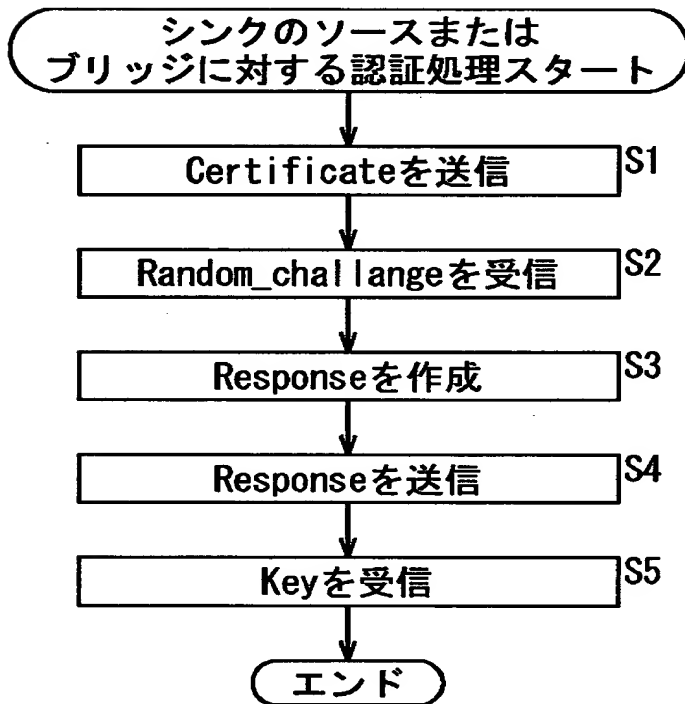
【図4】



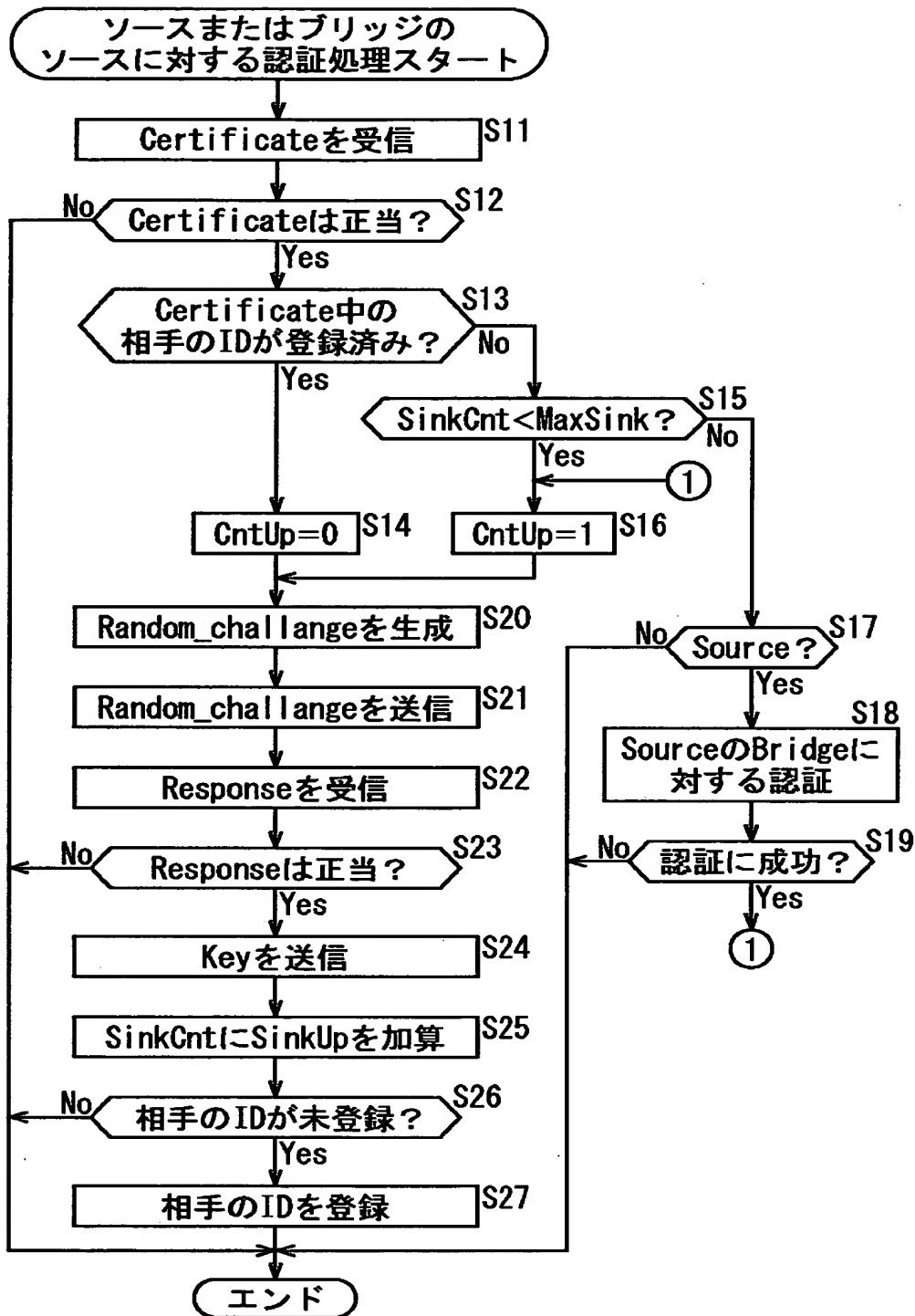
【図 5】



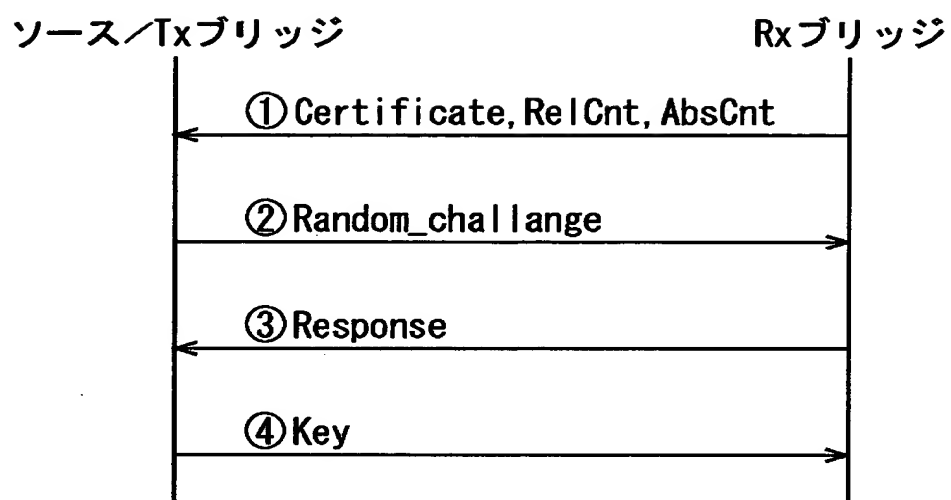
【図 6】



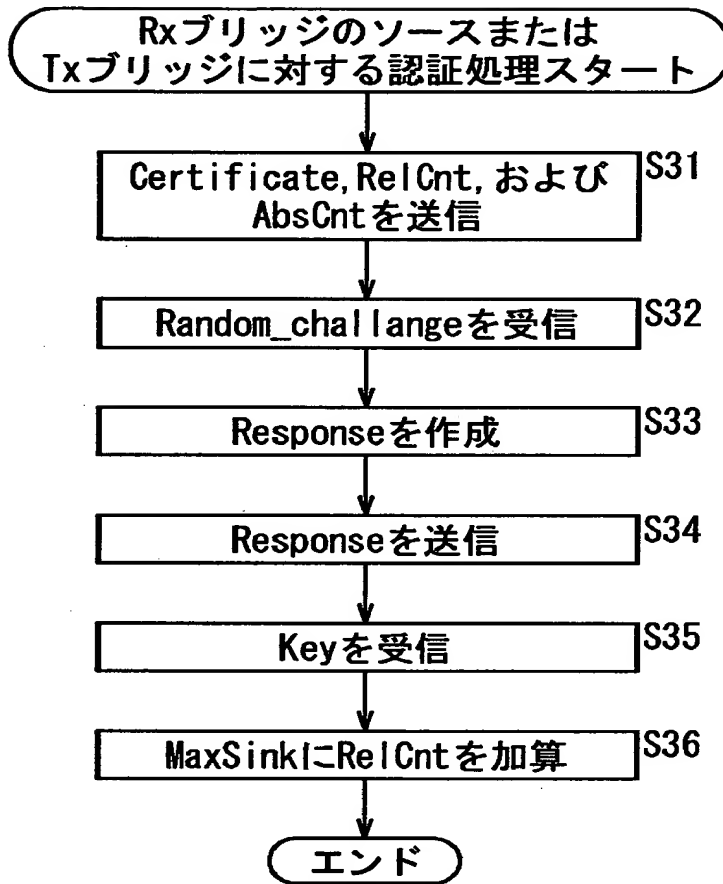
【図7】



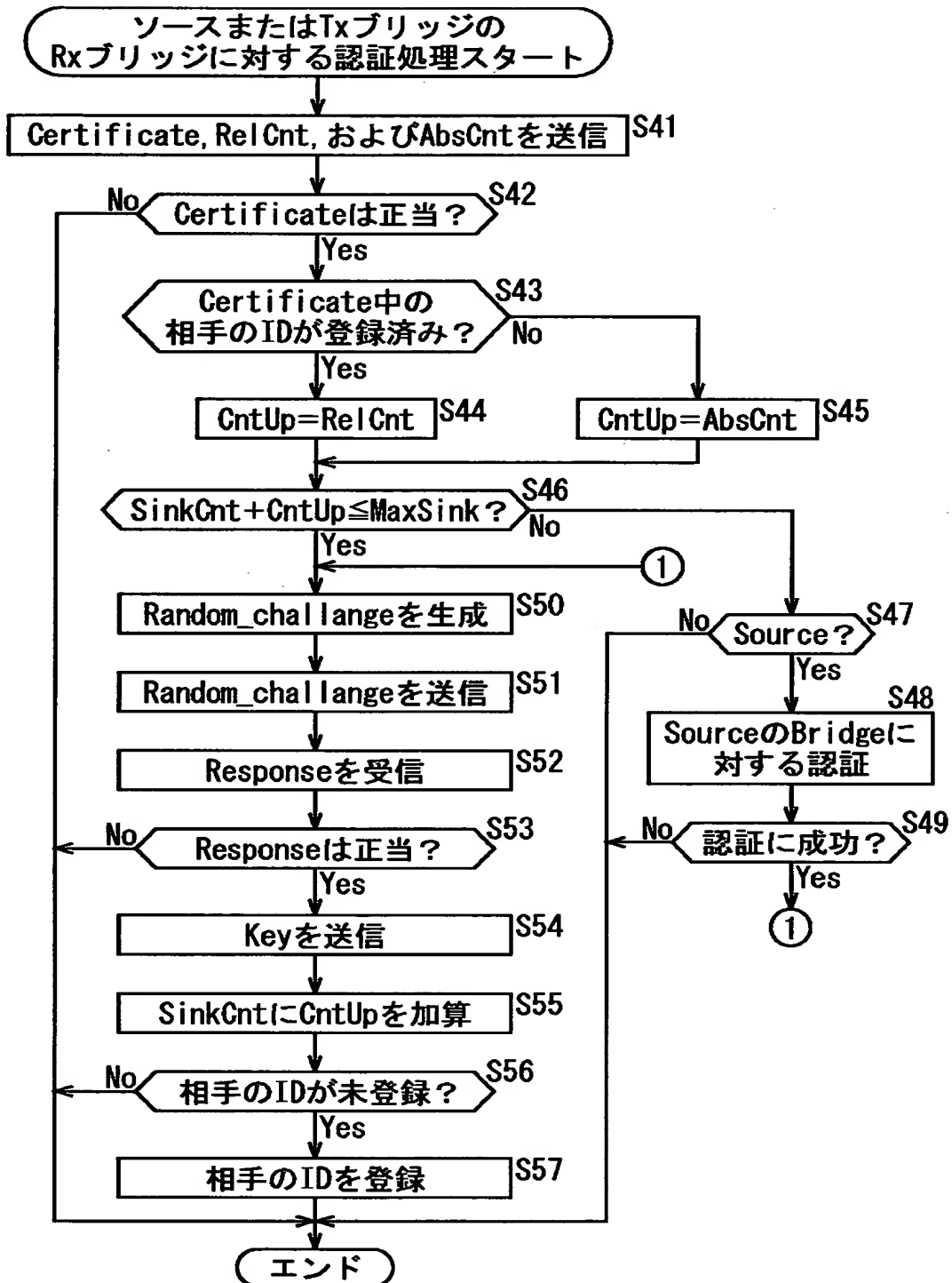
【図 8】



【図 9】



【図10】



【書類名】 要約書

【要約】

【課題】 コンテンツの利用を制限することができるようにする。

【解決手段】 ソース 1 は、シンク 2 - 1 よりコンテンツの送信要求を受けた場合、認証処理を行う。そして、認証に成功した場合、ソース 1 は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク 2 - 1 に送信する。シンク 2 - 1 は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことにより、コンテンツを受信することができる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2000-211787
受付番号	50000880907
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 7月17日

<認定情報・付加情報>

【特許出願人】

【識別番号】 000002185

【住所又は居所】 東京都品川区北品川6丁目7番35号

【氏名又は名称】 ソニー株式会社

【代理人】 申請人

【識別番号】 100082131

【住所又は居所】 東京都新宿区西新宿7丁目5番8号 GOWA西
新宿ビル6F 稲本国際特許事務所

【氏名又は名称】 稲本 義雄

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社